DISA

Defense Information Systems Agency
Department of Defense

NCES Service Security

Prepared by Booz Allen Hamilton

18 December 2006

Agenda

- **NCES Service Security Overview**
  - Introduction to Service Security
  - Open Standards
  - Major Components
  - How to integrate

The “Big” Picture

- The Department of Defense’s information sharing problems are more complex than any other organization in the world
  - 1,300,000 active duty, 660,000 civilian personnel, and 1,100,000 national guard and reservists who operate afloat and ashore in 163 countries across each of the world’s time zones[1]
  - Over 22,000,000 actively tracked veterans, retirees and dependents who require access to benefits and other information
  - Assets and liabilities that exceed those of Exxon, IBM, Ford and Wal-Mart combined[2]
  - Thousands and thousands of operational, in-use systems that contain relevant information used on a day-to-day basis

“In terms of people and operations, [the DoD is] busier than just about all of the nation’s largest private sector companies.” – www.defenselink.mil

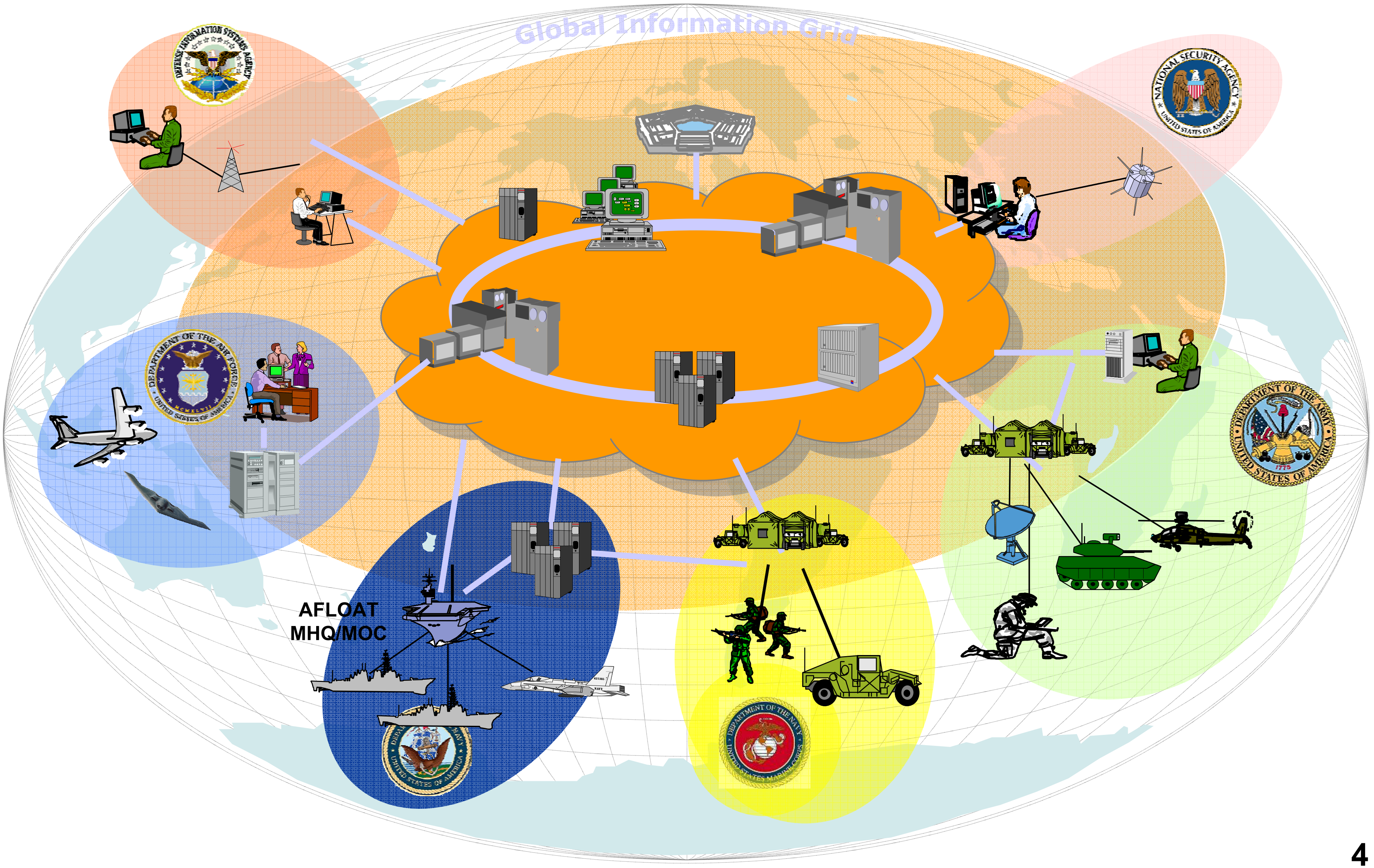
[1] http://www.defenselink.mil/pubs/dod101

[2] http://www.gcn.com/print/25_26/41802-1.html

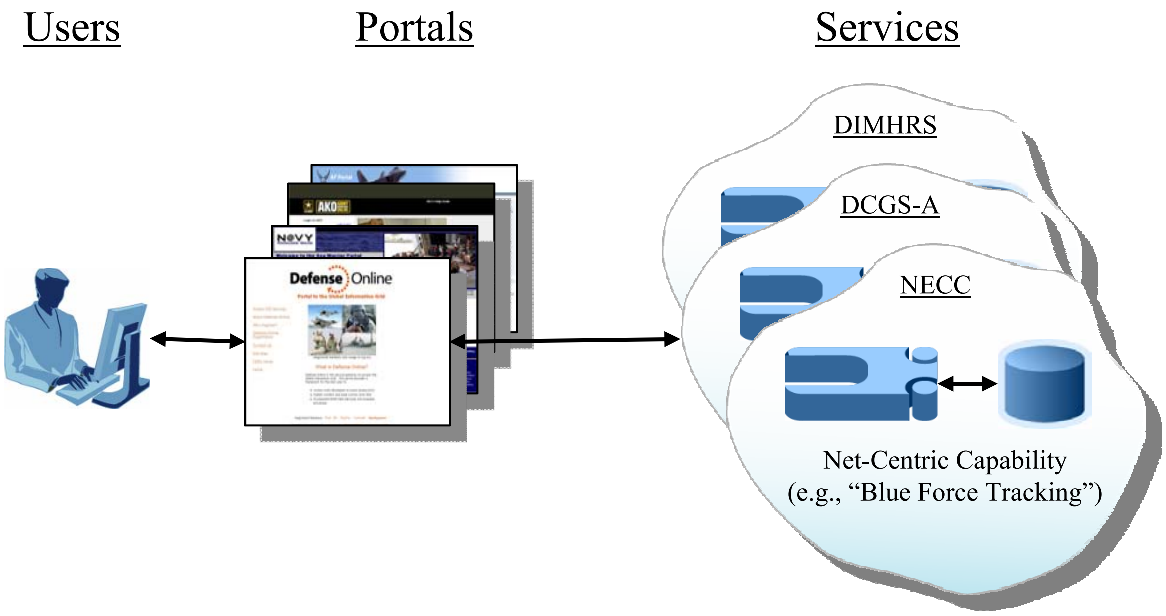
Accessing Shared Information

- Once information is shared, comprehensive mechanisms to control access to that information must be put in place
  - Everyone in the DoD shouldn’t be able to access every piece of shared information, since some information is sensitive
  - Therefore, information may be more or less broadly shared
- Deciding whether to allow access to shared information currently involves many manual and automated processes
  - For example, to verify that someone belongs to an appropriate organization, is a U.S. Citizen, has approval for special categories of information, or is specifically known to a community
- This “provisioning process” effectively segregates information along many lines, including mission area, topic, origin, classification, special compartments, or national affiliation

The Information Sharing End-State



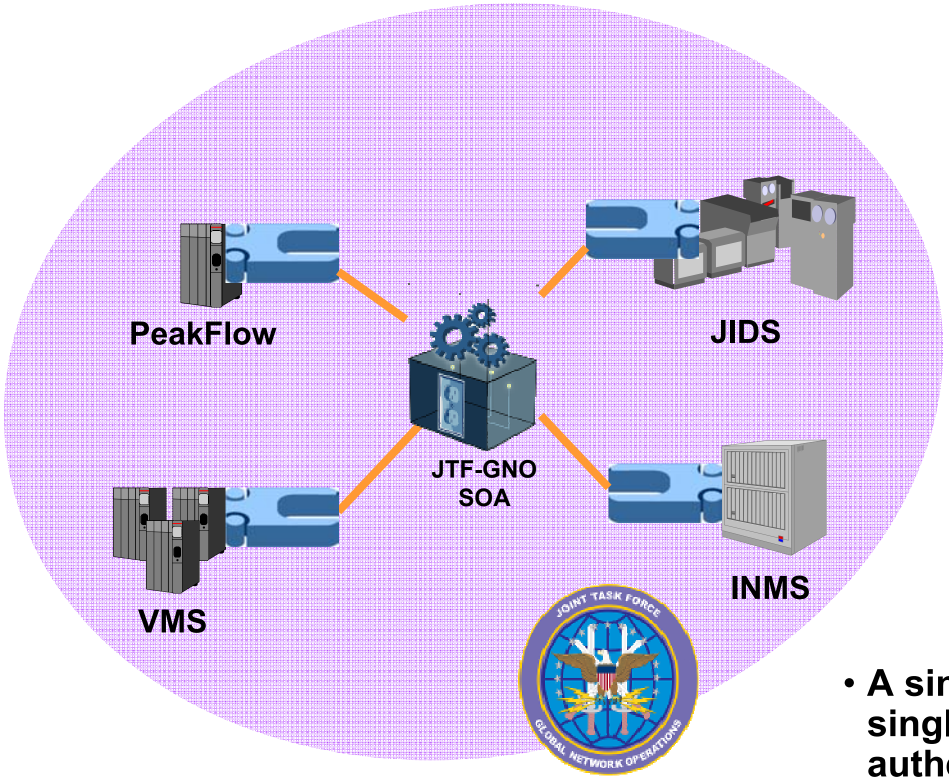
How Will Information Sharing Work?



- Portals provide a single point of entry to access information and capabilities.
- Programs of record share relevant information via "services" that can be discovered.
- These services can be used by DoD portals, systems and applications.
- Shared services must be secured to prevent unauthorized access.

The portals that display information and the services that share information must be protected from unauthorized access. Each has its own unique security requirements

Use Case: Sharing information within and across COCOMS, Services, and Agencies



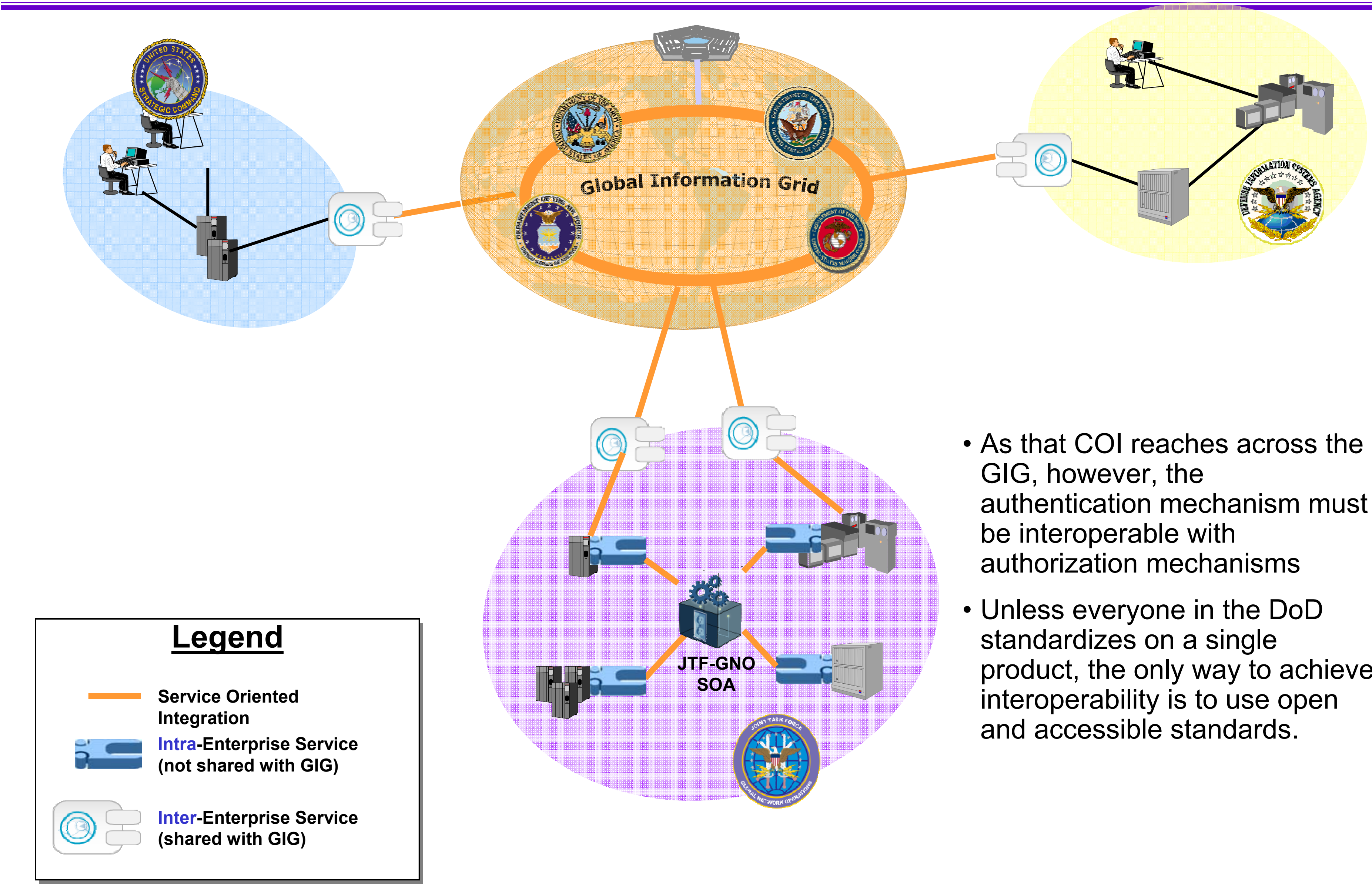
- A single enterprise may use a single product for authentication to all intra-enterprise data products

Legend

▬ Service Oriented Integration

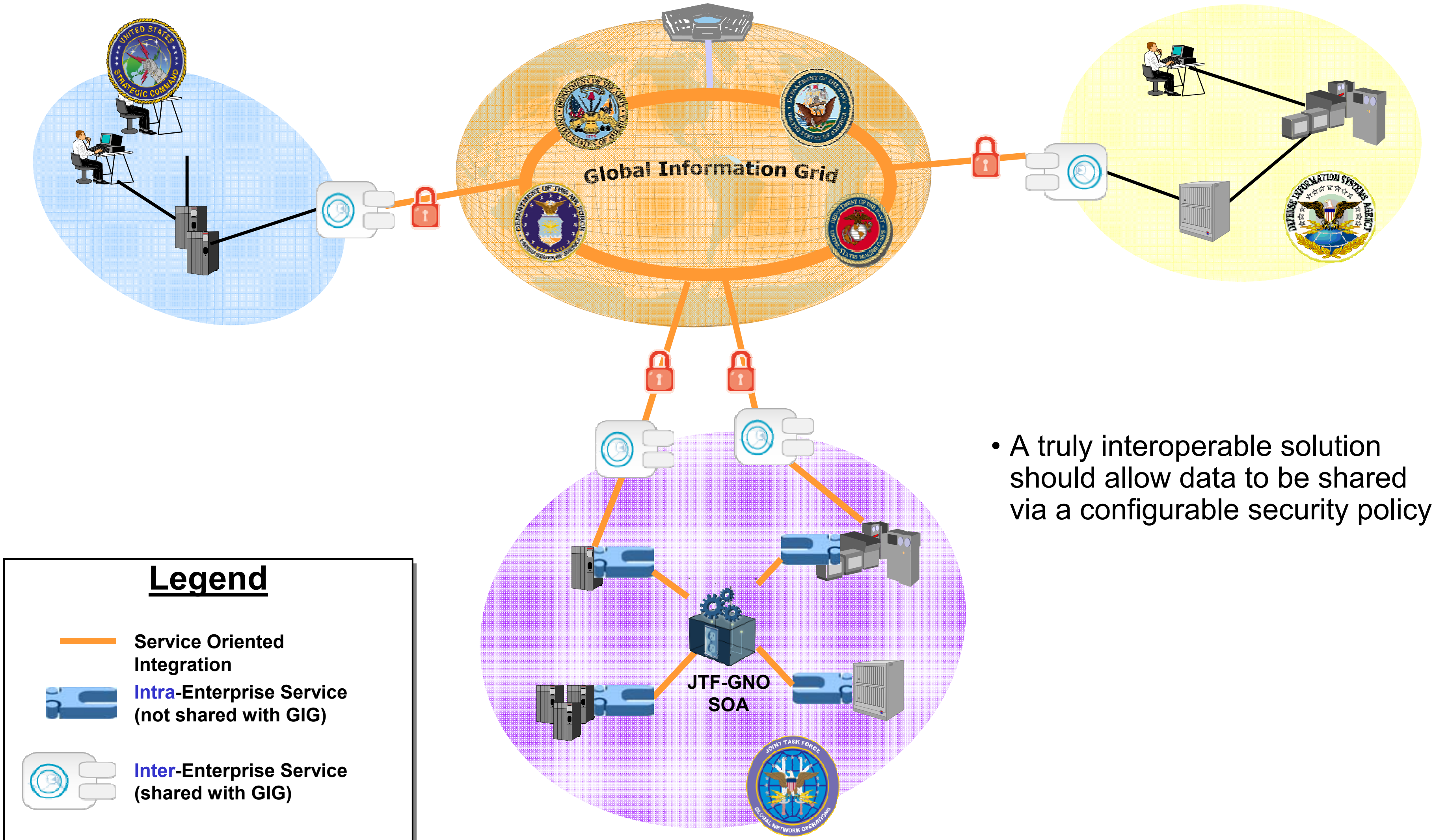
Intra-Enterprise Service (not shared with GIG)

Use Case: Sharing information within and across COCOMS, Services, and Agencies


Global Information Grid
JTF-GNO
SOA
Legend
Service Oriented Integration
Intra-Enterprise Service (not shared with GIG)
Inter-Enterprise Service (shared with GIG)

- As that COI reaches across the GIG, however, the authentication mechanism must be interoperable with authorization mechanisms
- Unless everyone in the DoD standardizes on a single product, the only way to achieve interoperability is to use open and accessible standards.

Use Case: Sharing information within and across COCOMS, Services, and Agencies


UNITED STATES STRATEGIC COMMAND
Global Information Grid
DEFENSE INFORMATION SYSTEMS AGENCY
JTF-GNO SOA
JOINT TASK FORCE GLOBAL NETWORK OPERATIONS

- A truly interoperable solution should allow data to be shared via a configurable security policy

Legend

🟧	Service Oriented Integration
▬	Intra-Enterprise Service (not shared with GIG)
◎	Inter-Enterprise Service (shared with GIG)
🔒	Protected by NCES Security Services

Competing and Complimentary Goals

For Information Providers …

- Ensure that shared information can only be accessed by a list of appropriate personnel which may vary depending on mission
- Have adequate assurance that the person or computer requesting shared information is who they claim to be
- Provide seamless access to information accessed from portals, user applications, Web services, handheld devices, and other information providers
- Automate, as much as possible, the process of granting and revoking access to shared information

For Information Consumers …

- Gain access to relevant and useful information as an unintended user
- Have the same access to information across all devices, network links, and ashore/afloat platforms
- Minimize the amount of time it takes to gain access to a new collection of shared information resources
- Ensure that all information is relevant, timely, and mission-oriented

Information providers generally favor protection and security, while information consumers want easy and automated access to shared data

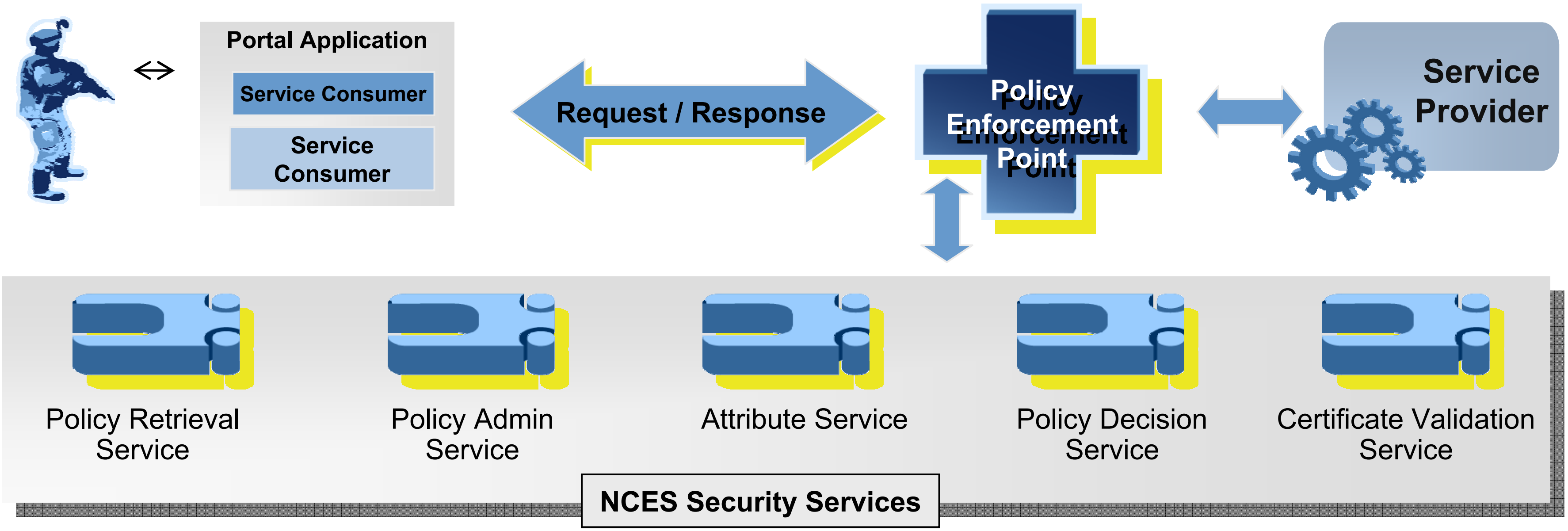
Agenda

- **NCES Service Security Overview**
  - Introduction to Service Security
  - Open Standards
  - Major Components
  - How to integrate

Security Service Components

Delivery Component	Description	Version
Security Services Architecture Document	Uses open standards from W3C, OASIS, and IETF to describe the system architecture, methodology, functionality, processing rules, and technology integration points necessary to protect services that share information	0.4.5
Security Services Reference Implementation	"Government Open Source" reference implementation that can be locally deployed for out-of-the-box security functionality	0.4.5
Security Services Software Development Kit (SDK)	Developer-level integration kit that eases integration for service providers and service consumers. Available for Java and .NET	0.4.5
Policy Console	Web-Based GUI console used to add, edit, delete and update security policies	0.4.5
Conformance Test Kit (CTK)	Web-based tool that validates how well a COTS or GOTS product meets the rules defined by the Security Services Architecture Document	0.4.5

Security Services: Detail View



Name	Protocol	Format	Standards Body
Service Request / Response	HTTP / SOAP	SOAP, WS-Security, XML-DSIG, SAML, WS-Addressing	OASIS / W3C
Attribute Service	SAML-P	SAML	OASIS
Policy Decision Service	SAML-P	SAML	OASIS
Certificate Validation Service	XKMS	XKMS /	W3C
Policy Retrieval Service	NCES-defined*	XACML	OASIS
Policy Administration Service	NCES-defined*	XACML	OASIS

*Not Accessible as an outside service

Supported Standards

Specification	Version	From
SOAP	1.1	W3C
WSDL	1.1	W3C
UDDI	3.0.2	OASIS
WS-Interoperability	Basic Profile 1.0	WS-I
XACML	1.2	OASIS
SAML	1.1	OASIS
XML-DSIG	Recommendation 2002-02-12	W3C
WSS	1.0 – SOAP Message Security 1.0 – X.509 Token Profile Draft 04 – SAML Token Profile	OASIS
WS-Addressing	2004-08-10 (Submitted to W3C)	Closed
XKMS	2.0	W3C

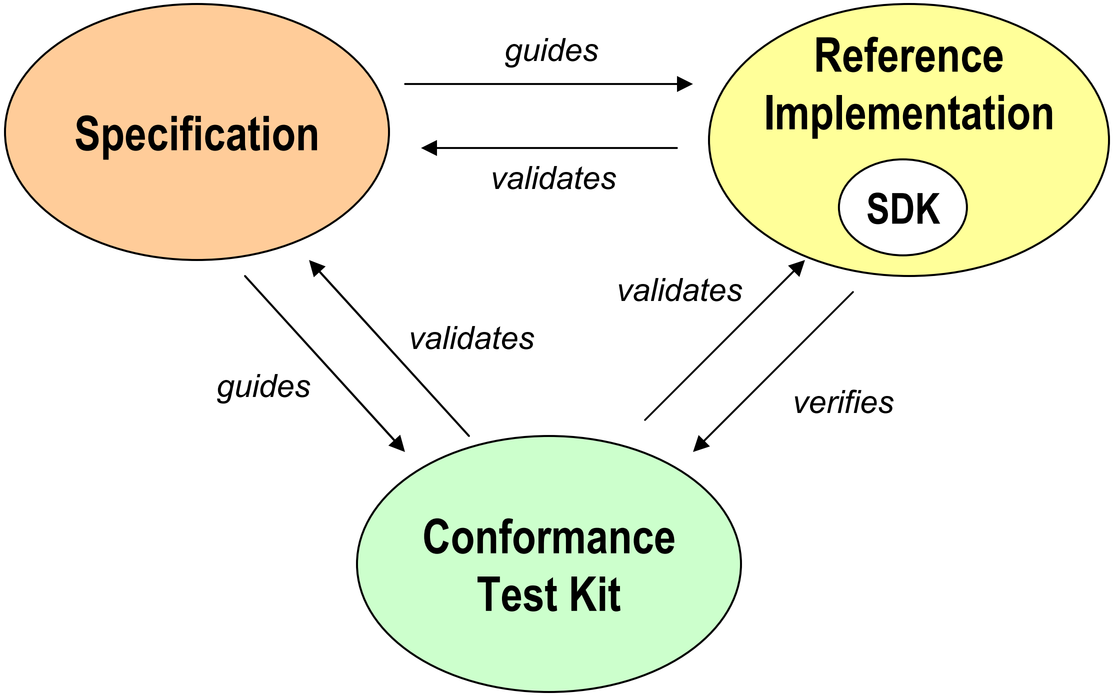
Agenda

- **NCES Service Security Overview**
  - Introduction to Service Security
  - Open Standards
  - Major Components
  - How to integrate

Security Service Components

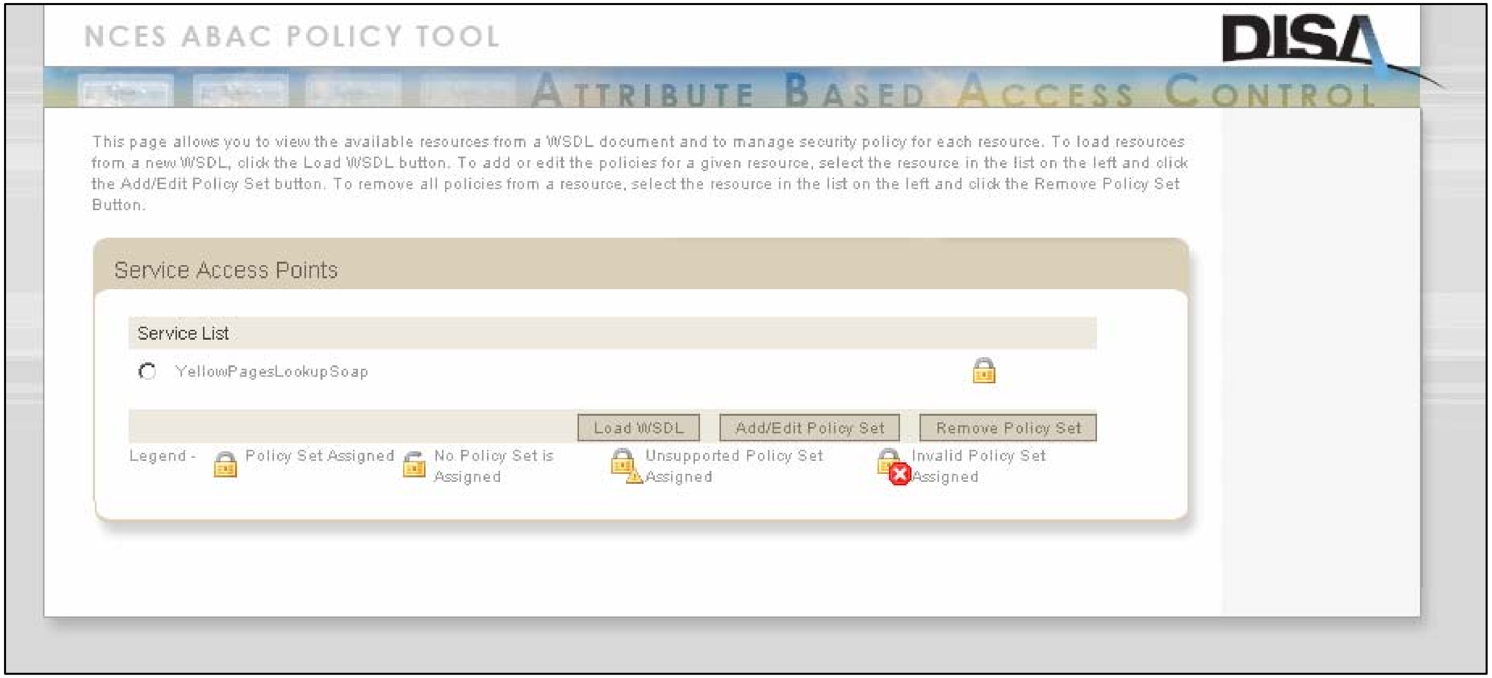
Delivery Component	Description	Version
Security Services Architecture Document	Uses open standards from W3C, OASIS, and IETF to describe the system architecture, methodology, functionality, processing rules, and technology integration points necessary to protect services that share information	0.4.5
Security Services Reference Implementation	"Government Open Source" reference implementation that can be locally deployed for out-of-the-box security functionality	0.4.5
Security Services Software Development Kit (SDK)	Developer-level integration kit that eases integration for service providers and service consumers. Available for Java and .NET	0.4.5
Policy Console	Web-Based GUI console used to add, edit, delete and update security policies	0.4.5
Conformance Test Kit (CTK)	Web-based tool that validates how well a COTS or GOTS product meets the rules defined by the Security Services Architecture Document	0.4.5

Complementary Activities



ABAC Policy Console

Security Policy Console



This page allows you to view the available resources from a WSDL document and to manage security policy for each resource. To load resources from a new WSDL, click the Load WSDL button. To add or edit the policies for a given resource, select the resource in the list on the left and click the Add/Edit Policy Set button. To remove all policies from a resource, select the resource in the list on the left and click the Remove Policy Set Button.

Service Access Points

Service List

○ YellowPagesLookupSoap

Legend - Policy Set Assigned · No Policy Set is Assigned · Unsupported Policy Set Assigned · Invalid Policy Set Assigned

- The Security Policy Console is a web-based tool that enables administrators to mange policies based on available attributes
- These policies can then be used to enforce Attribute Based Access Control (ABAC), which reduces manual account provisioning

What is ABAC?

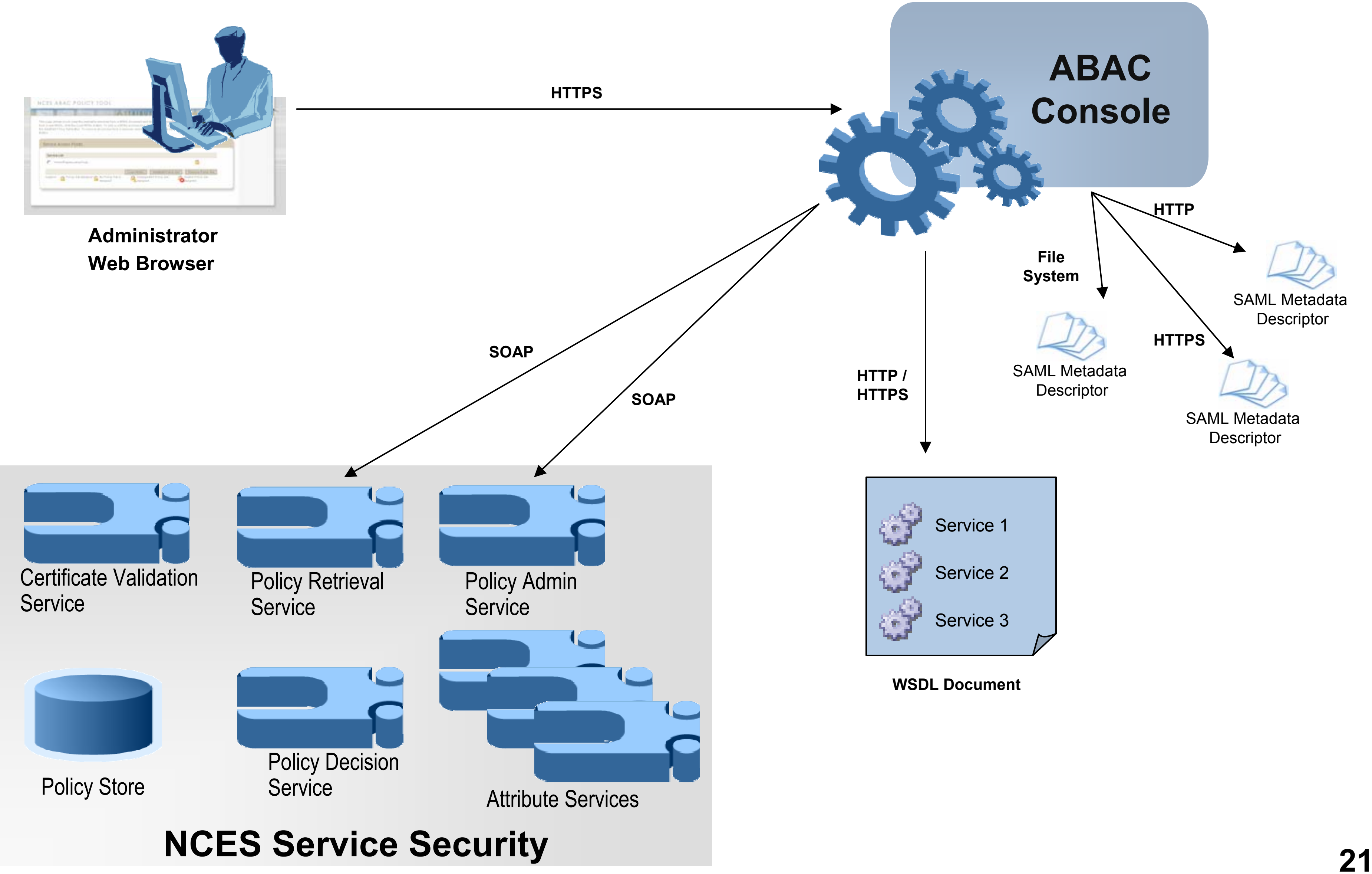
- **Attribute-Based Access Control (ABAC) is:**
  - A policy model that allows for authorization policy to be formulated based on an extensible notion of subject, resource, and other attributes

- **Three tenets of ABAC Authorization:**
  - An extensible notion of subject attributes
  - The use of various attribute types in policy rules
  - The use of resource attributes when specifying the applicability
    of a policy

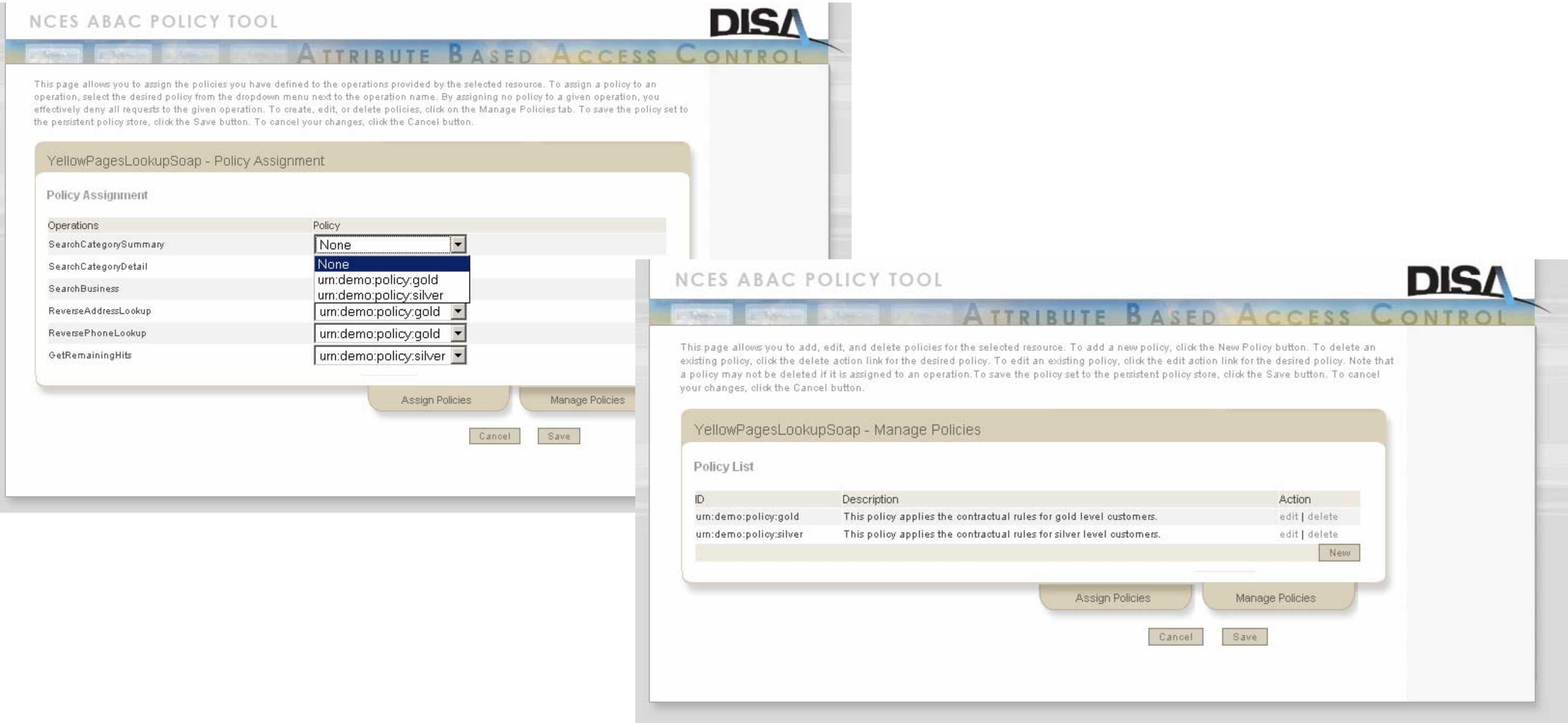
Attribute Based Access Control

- **ABAC Overview**
  - Indirect privilege management that bases privilege on many types of attributes. This obviates provisioning and allows run-time consideration of subject attributes.
  - Flexible enough for many longer-term needs, such as shared / personal file space or workspace, or Mandatory Access Control
  - Easier than other policy mechanisms to manage policy as the # of subjects and resources grows
  - Supports any attribute schema & assignments
  - Makes policies easier to manage

ABAC Console Architecture



Sample Screen Shots – ABAC Console



NCES ABAC POLICY TOOL

ATTRIBUTE BASED ACCESS CONTROL

This page allows you to assign the policies you have defined to the operations provided by the selected resource. To assign a policy to an operation, select the desired policy from the dropdown menu next to the operation name. By assigning no policy to a given operation, you effectively deny all requests to the given operation. To create, edit, or delete policies, click on the Manage Policies tab. To save the policy set to the persistent policy store, click the Save button. To cancel your changes, click the Cancel button.

YellowPagesLookupSoap - Policy Assignment

Policy Assignment

Operations	Policy
SearchCategorySummary	None
SearchCategoryDetail	
SearchBusiness	
ReverseAddressLookup	urn:demo:policy:gold
ReversePhoneLookup	urn:demo:policy:gold
GetRemainingHits	urn:demo:policy:silver

NCES ABAC POLICY TOOL

ATTRIBUTE BASED ACCESS CONTROL

This page allows you to add, edit, and delete policies for the selected resource. To add a new policy, click the New Policy button. To delete an existing policy, click the delete action link for the desired policy. To edit an existing policy, click the edit action link for the desired policy. Note that a policy may not be deleted if it is assigned to an operation.To save the policy set to the persistent policy store, click the Save button. To cancel your changes, click the Cancel button.

YellowPagesLookupSoap - Manage Policies

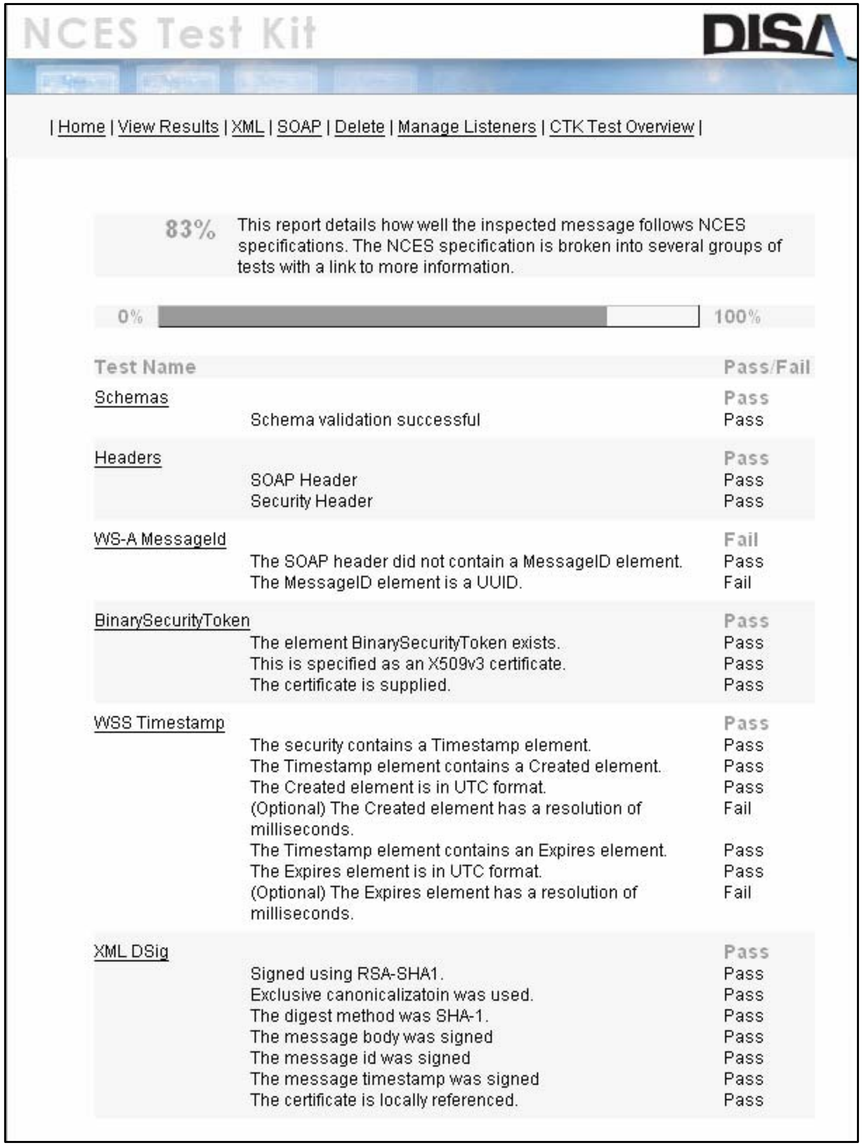
Policy List

ID	Description	Action
urn:demo:policy:gold	This policy applies the contractual rules for gold level customers.	edit | delete
urn:demo:policy:silver	This policy applies the contractual rules for silver level customers.	edit | delete

- **Assign Policies to operations on the resource**
- **Create, edit, and delete policies in the policy set**

Conformance Test Kit (CTK)

NCES Conformance Test Kit



NCES Test Kit

| Home | View Results | XML | SOAP | Delete | Manage Listeners | CTK Test Overview |

83% This report details how well the inspected message follows NCES specifications. The NCES specification is broken into several groups of tests with a link to more information.

0% 100%

Test Name		Pass/Fail
Schemas		Pass
	Schema validation successful	Pass
Headers		Pass
	SOAP Header	Pass
	Security Header	Pass
WS-A MessageId		Fail
	The SOAP header did not contain a MessageID element.	Pass
	The MessageID element is a UUID.	Fail
BinarySecurityToken		Pass
	The element BinarySecurityToken exists.	Pass
	This is specified as an X509v3 certificate.	Pass
	The certificate is supplied.	Pass
WSS Timestamp		Pass
	The security contains a Timestamp element.	Pass
	The Timestamp element contains a Created element.	Pass
	The Created element is in UTC format.	Pass
	(Optional) The Created element has a resolution of milliseconds.	Fail
	The Timestamp element contains an Expires element.	Pass
	The Expires element is in UTC format.	Pass
	(Optional) The Expires element has a resolution of milliseconds.	Fail
XML DSig		Pass
	Signed using RSA-SHA1.	Pass
	Exclusive canonicalizatoin was used.	Pass
	The digest method was SHA-1.	Pass
	The message body was signed	Pass
	The message id was signed	Pass
	The message timestamp was signed	Pass
	The certificate is locally referenced.	Pass

- The conformance test kit is a web-based toolkit that measures how well a COTS or GOTS product meets the NCES Security Specification
- Having a standard way to measure implementations allows for many different products, tools, and deployment options to remain interoperable
- The CTK provides testing coverage for the service request, the service response, as well as the five “core” services within NCES Security Services

Conformance Test Kit Overview

- **The Conformance Test Kit can be used in the following ways:**
  - Distributed to vendors or contractors that implement NCES security components. The CTK would measure compliance of COTS/GOTS tools.
  - Used by the NCES program to certify NCES components developed under contract comply with the NCES specification to ensure that contractual obligations have been met
  - The test kit can be used by the NCES program to determine if COTS products comply with the NCES specifications and are suitable for use in the NCES program
- **The rules validated by the CTK are derived from the NCES Security Architecture specification**

Testing Width vs. Depth

Conformance Testing “Width”

	Policy Enforcement Point	Policy Decision Service	Certificate Validation Service	Principle Attrribute Service	Policy Retrieval Service	Policy Admin. Service	Security Service Consumer
On-the-Wire Message Format	Web Service Message Inspection Tool						
Message Processing and Logic	PEP Test Harness	Web Service Message Processing and Logic Test Tool					N/A

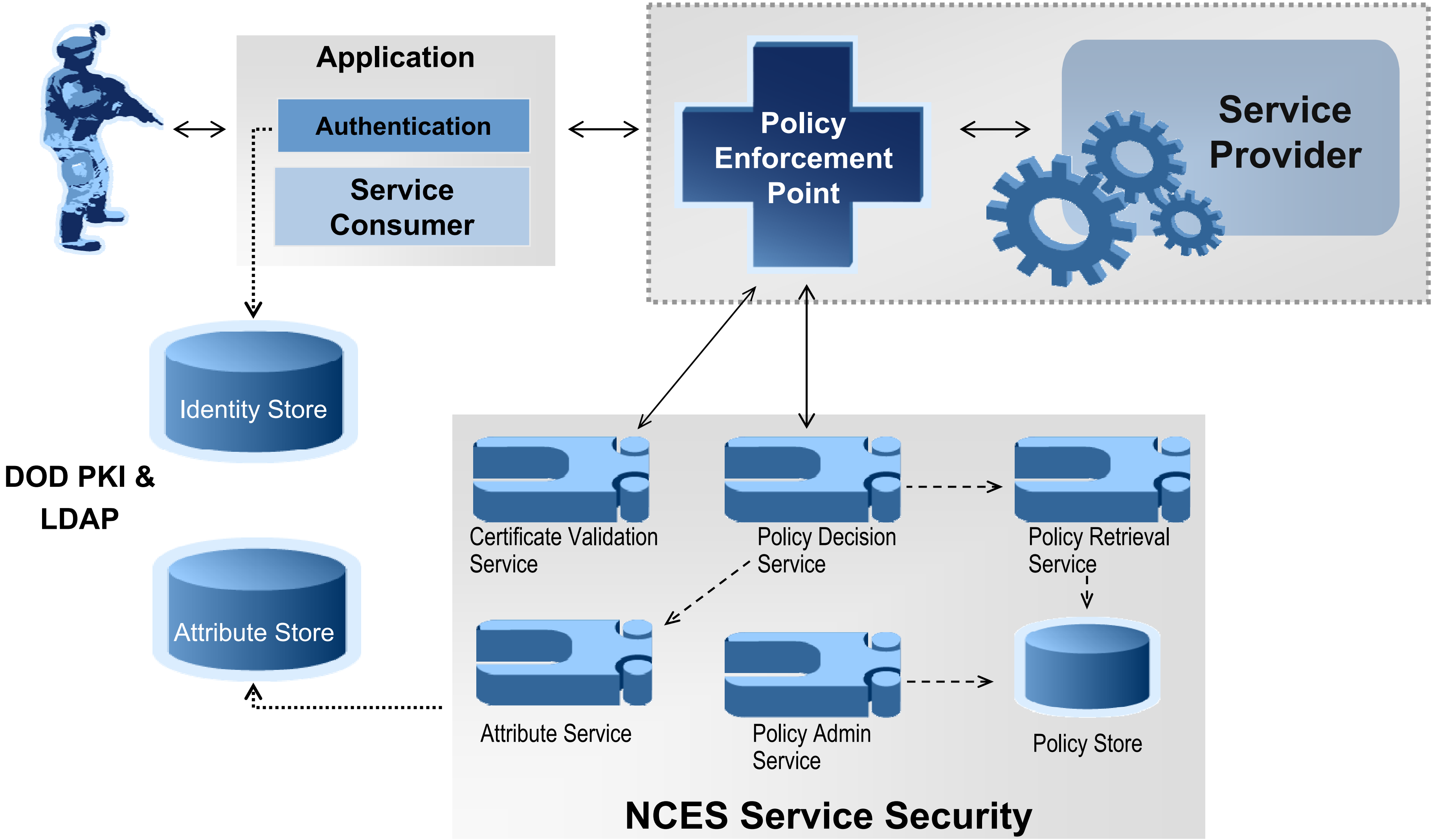
Conformance Testing “Depth”

NCES Security SDK

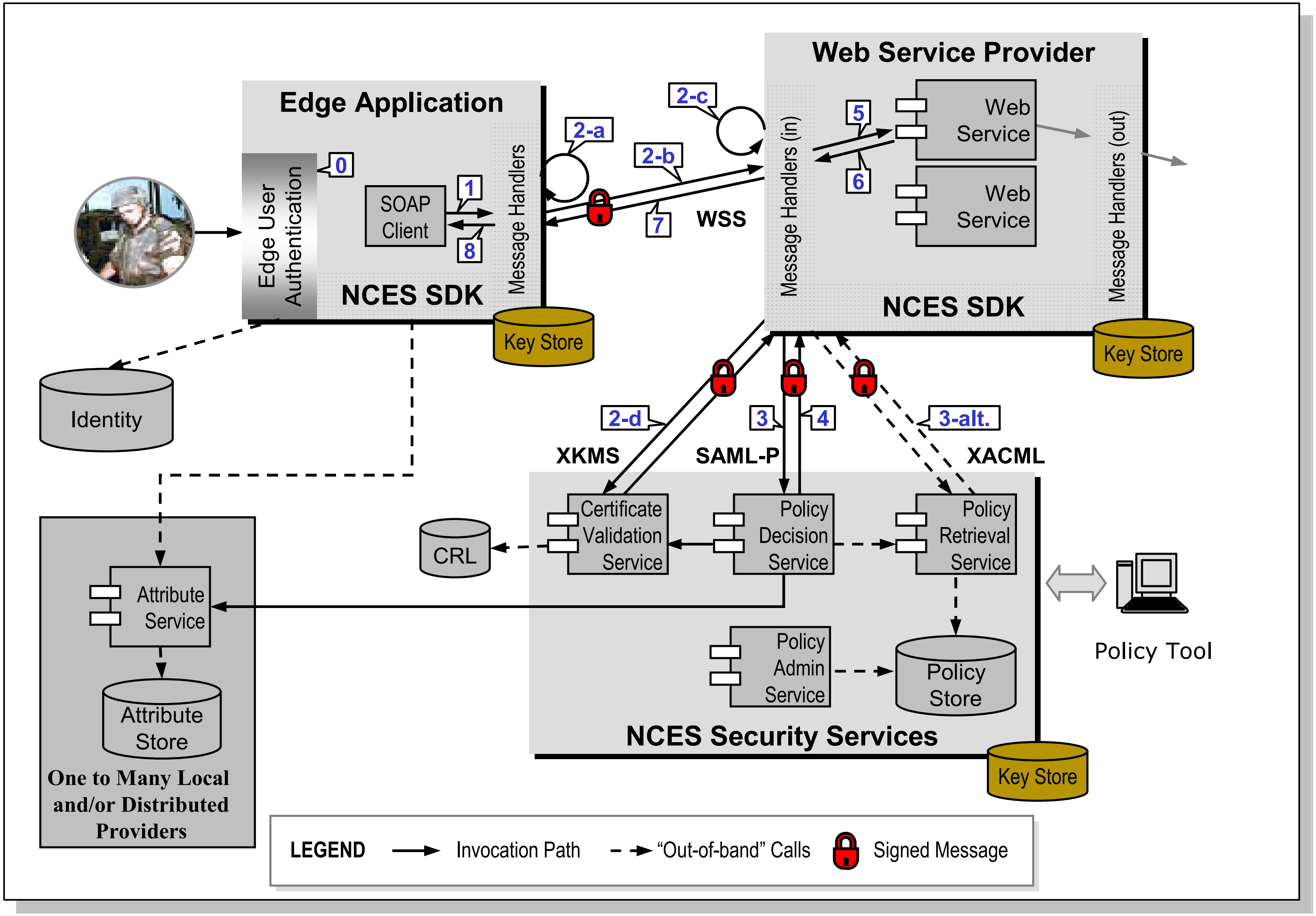
SDK Overview

- The NCES Security SDK is a Java and .NET integration toolkit that provides:
  - Client stubs to access the Security Enterprise Services
  - A software-based policy enforcement point that can protect shared Web services
  - A framework to create attribute services
- The Security SDKs can :
  - Provide access control for Web services
  - Enforce access control policies for protected Web service
  - Automatically format Web service messages to comply with the NCES Security Architecture (for interoperability)
  - Enable service consumers to call Web services protected by an NCES-compliant policy enforcement point

Logical Component Overview



Authorization Sequence w/ NCES SDK



LEGEND → Invocation Path - -→ "Out-of-band" Calls 🔒 Signed Message

NCES Security SDK

Additional Resources

- User’s Guides for Java and .NET SDKs
- Sample applications that show integration
- NCES Security Architecture Document
- WSDLs for NCES Security Services
- Available for use on NIPRNET / SIPRNET

Agenda

- **NCES Service Security Overview**
  - Introduction to Service Security
  - Open Standards
  - Major Components
  - How to integrate

How to integrate w/ Service Security

- **In order to use NCES Service Security, a service provider must first:**
  - Create a service that shares data
  - Publish the service to the NCES Registry
  - Create access policies for published services

- **There are three ways to protect a shared Web service:**
  - Download and configure the NCES SS SDK. As part of the SDK download, users will have access to:
    - SDK User's Guide & Release Notes
    - A sample Web service application
  - Build your own software Policy Enforcement Point (PEP) based on NCES specs
  - Configure a hardware-based PEP such as IBM's DataPower

www.disa.mil